SUNRED
SECURITY

INCIDENT RESPONDER COURSE MODULE

Incident responders are the frontline of cyber security. They are responsible for the alerting, containment and eradication of malicious activity.

Outcomes

Finding the confidence for incident response is typically forged in fire, however this isn't a healthy method for growth and often contributes to burnout.

This course gives security analysts the knowledge required to handle the incident response process. We focus on working through scenarios and hands on exercises to gain familiarity in a safe and fun environment.

Throughout the day we develop a incident response plan and finally work through executing the plan in exercises.

The Incident Responder Course Module covers:

We begin the day with an introduction to incident response and talk through the existing frameworks. From here we introduce our sample company and walk through some real world scenarios and how they map to the frameworks.

Working through some examples we investigate how incidents are first detected like through behavioral alerts, security event alerts, endpoint detection and user reports. After this we develop a shared classification of incidents and correlate prioritisation.

We work through each scenario and discuss the containment strategies. We use free and open source tools for lab environments to simulate compromise and eradication. If you would like to integrate the training with a commercial tool that your team uses then please contact us.

From here we focus on the recovery plans, ensuring the business can get back on track with minimal impact and making sure that nothing was missed. We follow up with mock post incident reviews and write up action plans.

Next we focus on incident communication and documentation. We will critique some documentation practices and write some procedures ourselves. Bringing communication methods into the documentation ensures a consistent and clear message to key stakeholders.

Finally we run through some incidents that have happened in the wild. Mapping either to your company or our sample company we run through the full incident response process as a team.